**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software
   1. What are the two types of modern encryption methods?

Symmetric-key encryption and asymmetric-key encryption.

1. Network policies, profiles

Network policies and profiles will be established for an organisation has employees to work on a single document through the internet. This is a basic step in making it harder for unauthorised users to access material.

1. Firewalls

Firewalls are another type of network protection, used to restrict access by outsiders to a network, as well as to protect confidential information, such as payrolls and personnel records, from employees not authorised to access it.

1. Antivirus software

Antivirus software can be used to prevent computer virus infections. This software detects the presence of viruses as the computer boots up, when an executable file is run, when documents are accessed or when files are copies.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.
   * + - Well-documented processes for communicating sensitive information
       - Use of passwords on documents that have sensitive information
       - Well-documented policy for the use of networked devices within the organisation

**Storage**

1. **Filenaming conventions**
   1. List the 3 types of information each document should include.
      * + - Data stamp: a data that indicates the timeliness of a document.
          - Variation: identifying which version of the file is saved.
          - Name: something meaningful that can identify the document.
   2. Give an example of a sequential file-naming convention.

DeathRecord 2015-11-08 V2.doc

1. **Location of files**
2. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

Full backup copies all of the files from a device to a storage medium.

* + 1. Differential backup

A differential backup copies only those files that have been changed since the last full backup.

* + 1. Incremental backup

Incremental backup is similar to a differential backup, the difference being that it uses more than two backup media, while a files that have been changed since that last incremental backup.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

It is a good practice to clearly label all backup media so that you know when the backup was made and what is on it. A log may also be kept by a systems manager recording backup dates

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

It is good practice that he location of backup files and whether any restorations have been made.

* 1. What is the grandparent-parent-child system?

It is the system indicate that the order of the copies that along the timeline.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving is essentially a process of copying files to long-time storage, then deleting them from the hard disk. Destruction involves deletion only.

* 1. What is a problem for ICT managers?

One problem for ICT managers, however, is determining which the most appropriate long-term storage medium to use is.

* 1. What is a legacy system?

An old system is generally referred to as a legacy system. These systems might run old databases on old servers or mainframes.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

The disposal of old equipment also poses a challenge for organisations.